IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2135
Serial No.	: 09/931,344	Examiner	: Ha, L.
Filed	: August 16, 2001	Conf. No.	: 2635
Title	: DEVICE TO PROTECT VICTIM SITES DURING DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Pursuant to 37 C.F.R. §41.41, Appellant will address the examiner's responses to Appellant's arguments in the order contained in the Examiner's Answer.

For those contentions of Appellant that the examiner did not address, Appellant relies on the arguments made in the Appeal Brief. Appellant points out for the Board's consideration that several of the dependent claims were argued separately, but the examiner elected not to respond to those arguments in the Examiner's Answer.

At the outset, the examiner contends that:

> **Throughout the Appeal Brief, appellant did not point to particular citations to specify what exactly that Pearson and Cheriton fails to teach or teach against that correspond to the claimed limitations being traversed. Appellant pointed to a couple of citations on pg.16-17, but throughout pgs.7-20 merely copy/paste examiner's rejection and passages from the prior arts without noting its column and lines relating to the traversal. Thus, examiner herein will respond in accordance with the claimed invention and to the best understanding in response to appellant's arguments and points discussed in this appeal brief.**[1]

Appellant to the extent that this argument is understood, disagrees. Appellant provided twenty footnote citations to the references, the examiner's action and to the specification in the Appeal Brief. Appellant included numerous embedded citations to the references in the body of

[1] Examiner's Answer page 20.

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: April 04, 2008

the arguments in the Appeal Brief. Therefore Appellant sufficiently pointed out and referenced those passages that supported Appellant's argument.

Therefore, to the extent that the examiner complains that Appellant had not sufficiently provided citations to the passages in the reference, Appellant disagrees because citations were provided. However, to the extent that the examiner's statement: "**Throughout the Appeal Brief, appellant did not point to particular citations to specify what exactly that Pearson and Cheriton fails to teach or teach against that correspond to the claimed limitations being traversed.**", requires Appellant to provide citations to places in the references and identify where the limitations of the claims are not taught, Appellant contends that this complaint is illogical and improper. The requirement is illogical because it asks Appellant to prove the negative. The requirement is improper because it is tantamount to an impermissible shift in the burden of production and persuasion that clearly rests on the examiner. Under 35 U.S.C. 102: "A person shall be entitled to a patent unless —." Indeed, "It is well established that the burden is on the PTO to establish a prima facie showing of obviousness, *In re Fritsch*, 972 F.2d. 1260, 23 U.S.P.Q.2d 1780 (C.C.P.A., 1972)."

Claim 1

The examiner makes several unsupported assumptions regarding what the prior art taught at the time of Appellant's invention. The examiner assumes for instance that: "... **Statistics can reasonably be interpreted as the relationship among groups of measurement and with relevance of similarities and differences in those relationships,**"[2] and also assumes that: "**As such, it is known in the art that DoS attacks are determined on their similarities and differences measured amongst the network traffic.**"[3] Neither of these newly formed assumptions is supported by the record. Appellant submits that the examiner should either support these assumptions by documentary evidence or withdraw them.

The need for these assumptions however is uncertain when the examiner admits that: "**As for Pearson, the communication device implements intrusion detection functionality via intrusion detector 160 and determining whether such communications comprise an attack or other security risk (i.e. DoS) by comparing to a list (col.8, lines 10-25 and col. 17, lines 8-22).**"[4] Neither Pearson nor the examiner explain how comparing statistics, which the examiner gives a broad, unsupported definition for, combined with the

[2] Examiner's Answer page 21.
[3] Id.
[4] Id., pages 21-23.

assumed knowledge that "**DoS attacks are determined on their similarities and differences measured amongst the network traffic,**"[5] can be used to raise an alert by comparing to a list [of attack signatures][6] or a list [of security risks],[7] as disclosed by Pearson. Neither of these features in Pearson are statistics, as called for by claim 1. It is not understood how Pearson would compare statistics to a list. How would that comparison be carried out and what meaning could be ascribed to such a comparison. The examiner's conclusion that: "**Pearson suggests the data collected in the communication device comprises attacks or other security risk (i.e. DoS) from monitoring the network in the gateway as collected statistics,**"[8] is therefore unsupported.

The examiner also argues that: "**Pearson discloses the communication device transmit a type of communication causing the alert (col.3, lines 5-8) and the RMC receive the signal or message indicative of an attack which then create a communication to the RMC (col.7, lines 59-62).**"[9] Appellant does not fully understand this reasoning. The examiner appears to state that the RMC creates a communication to itself, which is illogical and not supported by Pearson. This inconsistency notwithstanding, the examiner clearly overreaches arguing that: "**With Pearson able to determine whether such communications comprise an attack or other security risk (i.e. DoS) (col.8, lines 10-25 and col. 17, lines 8-22), obviously suggests sending statistics in the signal collected in the gateway to the control. Thus, the gateway communicating a signal to the control center (RMC) is not merely for signaling an alert, but is a message with statistics indicative of an attack.**"[10] In essence, the examiner has re-invented the primary reference.

Notwithstanding the fact that the primary references deals with attack signatures and not statistics collected in a gateway, and the examiner has yet to show where Pearson discusses statistics, the examiner now re-invents Pearson to argue that Pearson; "**obviously suggests sending statistics in the signal collected in the gateway**"[11], and that the "**the gateway communicating a signal to the control center (RMC) is not merely for signaling an alert, but is a message with statistics indicative of an attack.**"[12]

However, Pearson describes the alert signal as: **Monitoring engine 114 preferably also maintains a history of attacks on communication device 106 by recording incoming alert signals in a threat database 124 stored in the**

---

[5] Id., page 21.
[6] Pearson Col. 8, lines 18-19
[7] Id. Col. 17, line 22.
[8] Examiner's action page 22.
[9] Id.
[10] Id.
[11] Id.
[12] Id.

database farm."[13], and **"In an embodiment of the present invention, the alert signal contains priority information indicative of the seriousness of the attack. Based upon this priority information, the communication is stored in the corresponding threat database."**[14] Pearson describes the alert signal as identifying the type and seriousness of an attack. Nothing in Pearson supports the examiner unfounded assumption that the alert signal includes statistics.

The examiner also argues that: **"Further, Pearson discloses transmitting a wakeup signal to the RMC comprising diagnostic variables associated with the operations of the communication device and other parameter indicative of the state of operations of the communication devices where the RMC receives the signal and records the information contained in the signal and compares the information with a list (col. 3, lines 63-67 and col.12, lines 40-45)."**[15] The examiner attempts to equate or combine the features of the wakeup signal disclosed by Pearson with the alert signal. These are described by Pearson as different signals. While, neither of these signals has the claimed statistics, the wakeup signal is completely irrelevant to the features of claim 1.

The examiner conclusion that: **"Hence, once again Pearson suggests the signal includes data in order for the RMC to compare against with a list rather than just a carrier wave form utilized solely for warning or alerting."**[16], is totally without merit. This conclusion is erroneous, because it conflates two unrelated signals (the alert signal and the wakeup signal), attempts to interject an excuse to ignore the claim limitations[17] and improperly combines the two signals in a manner that would likely not be operative. In addition, the conclusion is erroneous because neither signal possesses the features of the claimed limitations.[18] In addition, to requiring the alleged combined signal, the examiner's conclusion requires this alleged combined signal to access a list of threats, which is also not directed to the claimed limitations.

The remaining argument that: **"Pearson discloses the violated rule is transmitted to the RMC ..."**[19] appears to be another attempt to read into Pearson "statistics collected in the gateway." However, it is clear that Pearson does not read on the claimed communication process because

---

[13] Pearson Col. 7, lines 5-8.
[14] Id. Col. 20, line 65 to Col. 21, line 2.
[15] Examiner's Action page 22.
[16] Id.
[17] The examiner's reference to carrier wave signal suggests an implicit excuse to ignore this limitation based on the recent Federal Circuit decision *In re Nuijten,*. 500 F.3d 1346, 1358 (Fed. Cir. 2007).
[18] The claims do not claim signals *per se*.
[19] Examiner's Action page 23.

Pearson neither describes nor suggests any device that communicates statistics collected in the gateway or the other elements of the communication process feature.

Appellant speculates that this reasoning may be the examiner's attempt to find the feature of: "a communication process … that receives queries or instructions from the control center," Appellant notes that there is no disclosed relationship between the alert signal and the wakeup signal of Pearson corresponding to the claimed feature of queries or instructions from the control center. Regardless of how the Board views Appellant's argument [20] concerning the communication process, which Appellant characterized as: "In essence, Pearson neither describes nor suggests that the control center queries the gateway for the statistical information."[21], as improperly construing this feature, it is clear that Pearson does not suggest the statistics.

The examiner has acknowledged that: "**Pearson is the primary art that teaches monitoring network traffic through the gateway and collecting statistics …** ,"[22] and therefore clearly agrees with Appellant that Cheriton would not otherwise cure the deficiencies in Pearson. Indeed, the examiner only used Cheriton to teach filtering. However, while Cheriton discloses filters, Cheriton does not cure the underlying deficiency in Pearson. Therefore, it is immaterial to patentability whether or nor the combination of Pearson and Cheriton teach the feature of inserting filters, as claimed in claim 1, because the remaining features of claim 1 are neither described nor suggested by any combination of Pearson in view of Cheriton.

The examiner elected not to present any answer to Appellant's arguments regarding Claims 2-15, many of which were argued separately. Therefore Appellant stands by the arguments set forth in the Appeal Brief.

---

[20] Appellant argued on Brief that: "Neither of these disclosed mechanisms however correspond to an arrangement by which a gateway collects statistical information pertaining to network traffic and receives queries from a control center to communication the statistics to the control center." (Appeal Brief page 9) The claimed feature is "a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center." Appellant believes that this characterization of the claimed feature is reasonable.

[21] Appellant's brief page 10

[22] Examiner's Action page 24.

Claim 29

Claim 29 is directed to a computer program product ... for protecting a victim site during a denial of service attack. Claim 29 includes instructions ... to monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic, communicate statistics collected in the computer device to a control center and filter out packets that the device or control center deems to be part of an attack.

Regarding the examiner's argument that: "**Statistics can reasonably interpret (sic) as the relationship among groups of measurement and with relevance of similarities and differences in those relationships,**"[23] Appellant has already challenged the examiner to support this newly presented assumption. Appellant's contentions that Pearson only describes attack signatures and that Pearson does not describe statistics, remains valid. (Cheriton is not relied on by the examiner to teach statistics see examiner's reasoning re: claim 1). Pearson defines attack signatures as:

> **More particularly, intrusion detector 160 inspects the unfiltered communications traveling over a specific network segment for the presence of predetermined attack signatures, by comparing to a list 170 of known attack signatures. Attack signatures are activity patterns indicative of undesirable activity, i.e., evidence that an unauthorized communication has been received. Examples of attacks include Denial of Service (DoS) attacks, unauthorized access attacks, attempts to modify data or kill programs, protocol violations, and repeated access attempts indicating malicious intent.**[24]

Notwithstanding what Pearson actually teaches, the examiner concludes that: "**Thus, the DoS are determined on similarities and differences measured amongst the network traffic.**"[25] In Pearson, DoS attacks are detected by comparing attack signatures to a list of known attack signatures. (See quote above.) The examiner overlooks or ignores that claim 29, like claim 1, while being directed to statistics, also includes the feature of "instructions ... to "monitor network traffic sent to the victim site and measure heuristics of the network traffic to provide statistics on the network traffic." Claim 29 requires instructions that "measure heuristics of the network traffic to provide statistics on the network traffic." No combination of Pearson and Cheriton suggests

---

[23] Id. page 26.
[24] Pearson, Col. 8, lines 18-24.
[25] Examiner's Action page 26.

instructions to measure heuristics of the network traffic to provide statistics on the network traffic," as claimed.

As with Claims 2-15, the examiner elected not to present any answer to Appellant's arguments regarding, Claims 30-39, many of which were grouped with claims 2-15, but in effect are argued separately because their base claim 29 was argued separately from claim 1. Therefore Appellant stands by the arguments set forth in the Appeal Brief.

Claim 16

The examiner correctly noted that appellant did not address the rejection of independent claim 16 separately, but rather argued it together with independent claim 1.

As with Claims 2-15, the examiner elected not to present any answer to Appellant's arguments regarding, Claims 17-28, many of which were argued in groups containing claims 2-15. Therefore, Appellant stands by the arguments set forth in the Appeal Brief.

For these reasons, and the reasons stated in the Appeal Brief, Applicant submits that the final rejection should be reversed.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 4/4/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906